# Hacking Device through Voice Interfaces

## General Description

Voice activation capabilities have been added to many computerized devices in recent years. From dedicated devices, (e.g. Amazon Alexa) through software agents for dedicated devices (e.g. Apple’s Siri) to software agents for general hardware (e.g Microsoft Cortana) – they all open a new interface to computerized devices by way of voice. While this new interface clearly brings a reward to our daily interaction with machines, it also holds a risk – which has had only recently been explored.

Voice interfaces - and virtual assistants associated with them - seem to pose two main threats to our computing environments: new delivery methods and authorization loopholes. The former is the ability to deliver malicious instructions through the air or through new formats of files. The latter is the ability to bypass validation mechanism that are missing when virtual assistant invokes certain functionality. Interesting examples of both already exist.

## Project Goals

Students will read existing literature regarding voice related cyber attacks and pick up a topic to dive into. Options include:

* Compromising locked computers through voice interfaces
* Delivering malicious instructions through voice files
* Abusing sound in web sites to compromise user accounts
* Reverse engineering of virtual assistant’s network protocol and local behavior

Deliverable is expected to include a working demo or a tool

## Prerequisites

* Programming experience
* Computer Security knowledge
* Understanding Internet structure and application
* Creativity and hands on capabilities

## Suggested Reading

* <https://assets.documentcloud.org/documents/3987864/Dolphinattack.pdf>
* <https://www.usenix.org/system/files/conference/woot15/woot15-paper-vaidya.pdf>
* <https://www.georgetown.edu/sites/www/files/Hidden%20Voice%20Commands%20full%20paper.pdf>
* <https://www.youtube.com/watch?v=Yf0WJQfGQoY>
* <https://nakedsecurity.sophos.com/2017/04/18/burger-king-triggers-ok-google-devices-with-tv-ad/>